UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/187,700	11/06/1998	HIROYUKI KOBAYASHI	3408.62676	3400

24978 7590 12/11/2003

GREER, BURNS & CRAIN
300 S WACKER DR
25TH FLOOR
CHICAGO, IL 60606

EXAMINER	
MEISLAHN, DOUGLAS J	

ART UNIT	PAPER NUMBER
2132	26

DATE MAILED: 12/11/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

PRG

Office Action Summary	Application No	Applicant(s)	
	09/187,700	KOBAYASHI ET AL.	
	Examiner	Art Unit	
	Douglas J. Meislahn	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 November 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14 and 16-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14 and 16-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 20 November 2003 that cancelled claim 15, added claim 20, and amended claim 11.

Response to Arguments

2. Applicant's arguments filed 20 November 2003 have been fully considered but they are not persuasive. Applicant did not file any arguments, *per se*. The argument section refers back to the arguments made in paper number 21, amendment E. The advisory action gave a rebuttal to those arguments. As the application has been RCEed, finality cannot be withdrawn.

3. Amendment E discusses three preliminary matters, the first two of which do not currently pertain to the patentability of the claims. The last preliminary matter alleges that the examiner has yet to adequately explain how either Kaufman or Ganesan disclose, together or alone, generating different key data for each of a plurality of unit storage areas on a storage medium. As the examiner explained in the final office action mailed 17 June 2003 (paper 20), the claim language's use of "for" can broadly be read to include a key being "for" a storage area after a program that is encrypted with that key is stored in the area. As such, Ganesan's symmetric key reads on the key "for" a specific storage area. The rejection in paper 20 (second paragraph of section 7) specifically explains the relationship of Ganesan to the claim language.

4. Applicant feels that the examiner both mischaracterized a previous argument and incorrectly ascribed a feature (indirect password encryption) to the prior art. The

examiner does not agree that any of applicant's arguments have been mischaracterized. Ganesan clearly shows indirect public key encryption (see figure 4, elements 330, 340, 380, and 390). The teachings of Kaufman render obvious a switch from indirect public-key to indirect password encryption.

5. Applicant argues that the examiner mischaracterizes the claim language "each of a plurality of storage areas". Again, the examiner has interpreted the scope of the claims broadly. In Ganesan, data is encrypted with a key and then stored in a storage area along with a cryptogram of the symmetric key. The symmetric key is random, and its generation reads on generation of a key for a specific unit storage area because of the breadth of "for". The step of encrypting with a password is covered by the combination of Ganesan and Kaufman. Ganesan shows writing the cryptogram to a storage medium. Once data is written to a data storage area, the encrypting key is "for" that storage area. The claims would not allow for this interpretation if the claims specifically mandated that an encryption key be selected for a piece of data based on where that piece of data is to be stored. Judging from applicant's arguments, this embodiment is within the application's scope.

6. Applicant notes that the examiner has said that the private key operates as a password. While correct, this is immaterial to the patentability of the claims. Private keys are used in public key cryptosystems – they are privately held by one individual and decrypt data that has been encrypted using corresponding public keys. A private key is thus different than symmetric key, which is used to decrypt or encrypt data that has been encrypt or will be decrypted with the same symmetric key.

7. Applicant raises an interesting issue relating to access to a database versus user-accessed data on a database. However, as this has not been related to specific claim language, the examiner does not see how it relates to the patentability of the claims.

Claim Objections

8. Claim20 objected to because of the following informalities: delete "a" in the second to last line of the claim. Appropriate correction is required.

Claim Rejections - 35 USC § 112

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 1-14, 16, 17, and 20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

11. Claim 1 recites the limitation "said key data generating step" in the eleventh line, "said encrypted key data" in the sixteenth line, "said data encrypting step" in the seventeenth line, and "and said data decoding step" in the last clause. There is insufficient antecedent basis for this limitation in the claim. Change "said" to "the". This same correction applies to the other maladies.

12. Claim 8 recites the limitation "said encrypted key data" across lines 16 and 17. There is insufficient antecedent basis for this limitation in the claim.

13. Claim 20 recites the limitation "said encrypted key data" in line 4, "said generated random key data" across lines 5 and 6, "said encrypted data" in line six, "said decoded

encrypted key data" across lines 11 and 12, "said key data generating step" in line 13, "said data encrypting step" in line 20, and "said data decoding step" in line 23. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15. Claims 1, 6-8, and 13-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ganesan (5748735) in view of Kaufman (6178508).

Ganesan's fourth figure shows a symmetric key being generated in element 330. Subsequently, this key is encrypted. In element 390, the encrypted symmetric key and data encrypted with that symmetric key are stored. With the exception of the password stipulation, clause one is hereby rendered obvious. Clause two is anticipated by elements 390 and 380. Step 580 in figure 5 shows reading the encrypted symmetric key from a storage medium, meeting the limitations of the third clause. The next step, element 585, anticipates the non-password portion of clause four. Element 590 anticipates clause five.

In lines 27-31 of column 6, Ganesan stipulates that the encrypted file and encrypted key are stored on an associated memory device. This reads on generating a key for a storage area. As is apparent from the abstract, the intent of Ganesan is to

provide storage for a multitude of files. The writing of the encrypted key to the memory device has already been described.

Ganesan says that the symmetric key is encrypted with a private key, not a password, although there are some functional similarities between the two: only the holder should know both, and both are often used for authentication. There are also several differences, such as the former being used in a public key cryptosystem and the latter, when acting as a key, being used in a symmetric key cryptosystem, as shown by Kaufman in lines 14-24 of column 6. Another difference is that passwords can generally be easily remembered while private keys practically require storage on a computer readable medium. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use a password as taught by Kaufman to encrypt the symmetric key in Ganesan. As is evident from Kaufman's exclusive-OR operation, this would conserve processing power.

Claim 6 is covered by Kaufman's plurality of passwords and quorum needed to decrypt. See columns five and six. Repeated encryptions of a secret are well-known and thus claim 7 is anticipated.

16. Claims 2 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ganesan and Kaufman as applied to claim 1 above, and further in view of Cruts et al. (4780905).

Ganesan and Kaufman show a system in which a symmetric key is encrypted with a password and stored with data that the symmetric key has encrypted. The key and data are associated with the memory device in which they are stored. They do not

say that the key is generated per the logic sector of the storage medium. In lines 46-48 of column 2, Cruts et al. say that a decryption key is based on a formula that uses the disc address of data. In lines 24 and 25 above, they say that this saves the user from needing to know and remember the encryption key. This is not to say that the encryption key is deleted (see abstract). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to associate the keys in Ganesan with the memory device on which they were to be stored by forming them according to an algorithm based on the address of the data, thereby saving the user from needing to remember the encryption keys.

17. Claims 3, 4, 10, and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ganesan and Kaufman as applied to claim 1 above, and further in view of Schneier (*Applied Cryptography*).

Ganesan and Kaufman show a system in which a symmetric key is encrypted with a password and stored with data that the symmetric key has encrypted. The key and data are associated with the memory device in which they are stored. They do not say that new symmetric keys are generated each time data is written to a spot in the memory device. On pages 6 and7, Schneier mentions the ciphertext-only attack, which relies on knowledge of multiple ciphertexts encrypted with the same encryption key. One obvious response to this is to use keys but once, which, depending on the algorithm, can verge on a one-time pad, which is a perfectly secret algorithm. Therefore it would have been obvious to a person of ordinary skill in the art at the time the

invention was made to generate new keys, as suggested by Schneier, every time data is written to a memory device in Ganesan.

Neither Kaufman nor Ganesan say that the symmetric key is made by combining a predetermined number of pieces of random data. On page 173, Schneier says that good keys are random-bit strings generated by an automatic process. One way to achieve this is to generate the key from a reliably random source. This source reads on applicant's predetermined number of pieces of random data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to generate the symmetric key in Kaufman using random pieces of data as taught by Schneier in order to have a "good" key.

18. Claim 5 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ganesan and Kaufman as applied to claim 1 above, and further in view of Blakley, III et al. (5677952).

Ganesan and Kaufman show a system in which a symmetric key is encrypted with a password and stored with data that the symmetric key has encrypted. The key and data are associated with the memory device in which they are stored. They do not present a system by which passwords are changed. In lines 6-25 of column 7, Blakley, III et al. show a method of changing a password that consists of decrypting data with the old password and re-encrypting it with the new password. In Blakley, III et al., these two steps occur simultaneously. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to change passwords in the

system of Ganesan and Kaufman according to the method of Blakley, III et al., thereby letting users update their passwords.

19. Claims 1, 2, 6-9, 13, 14, and 16-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bertina et al. (5682027).

From line 61 of column 1 through line 9 of column 2, Bertina et al. present a method of protecting data that includes encrypting the data with a key, where the key is based on the memory area in which the data is to be stored. The keys are stored in a security module. While not explicitly recited in Bertina et al., the security module could obviously be part of the device that contains the memory areas. The keys for the memory areas have been generated. As such, the step of generating different random key data for each of a plurality of unit storage areas is anticipated, as are the sub-steps of encrypting and decoding data with the random key corresponding to the unit storage area in which the data is stored. Writing the key data to the device is also rendered obvious. Bertina et al. do not say that the keys in the security module are encrypted with a password. Kaufman, in lines 14-24 of column 6, teaches protecting keys by encrypting them with a password. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to protect the keys in Bertina et al.'s security module by encrypting them with a password, as taught by Kaufman.

Claim 6 is covered by Kaufman's plurality of passwords and quorum needed to decrypt. See columns five and six. Repeated encryptions of a secret are well-known and thus claim 7 is anticipated.

20. Claims 3, 4, 10, and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bertina et al. and Kaufman as applied to claim 1 above, and further in view of Schneier (*Applied Cryptography*).

Bertina et al. and Kaufman show a system in which a symmetric key is encrypted with a password and stored with data that the symmetric key has encrypted. The key and data are associated with the memory device in which they are stored. They do not say that new symmetric keys are generated each time data is written to a spot in the memory device. On pages 6 and 7, Schneier mentions the ciphertext-only attack, which relies on knowledge of multiple ciphertexts encrypted with the same encryption key. One obvious response to this is to use keys but once, which, depending on the algorithm, can verge on a one-time pad, which is a perfectly secret algorithm. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to generate new keys, as suggested by Schneier, every time data is written to a memory device in Bertina et al.

Neither Kaufman nor Bertina et al. say that the symmetric key is made by combining a predetermined number of pieces of random data. On page 173, Schneier says that good keys are random-bit strings generated by an automatic process. One way to achieve this is to generate the key from a reliably random source. This source reads on applicant's predetermined number of pieces of random data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to generate the symmetric key in Kaufman using random pieces of data as taught by Schneier in order to have a "good" key.

21. Claim 5 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bertina et al. and Kaufman as applied to claim 1 above, and further in view of Blakley, III et al. (5677952).

Bertina et al. and Kaufman show a system in which a symmetric key is encrypted with a password and stored with data that the symmetric key has encrypted. The key and data are associated with the memory device in which they are stored. They do not present a system by which passwords are changed. In lines 6-25 of column 7, Blakley, III et al. show a method of changing a password that consists of decrypting data with the old password and re-encrypting it with the new password. In Blakley, III et al., these two steps occur simultaneously. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to change passwords in the system of Bertina et al. and Kaufman according to the method of Blakley, III et al., thereby letting users update their passwords.

Conclusion

22. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Shear (4827508) presents a portable storage device that has stored thereon a plurality of databases, each encrypted with its own key, and the keys. The keys can be encrypted (lines 1-2 of column 5).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J. Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached on between 9 AM and 6 PM, Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Douglas J. Meislahn
Examiner
Art Unit 2132

DJM